UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF PENNSYLVANIA

KYLIE BRENEMAN and BRANDY ARROYO-RYAN, individually and on behalf of all others similarly situated, Plaintiffs, v. KEYSTONE HEALTH, Defendant.	Case No. **CLASS ACTION COMPLAINT** JURY TRIAL DEMANDED

Plaintiffs Kylie Breneman and Brandy Arroyo-Ryan ("Plaintiffs"), individually and on behalf of all others similarly situated (collectively, "Class members"), by and through their attorneys, bring this class action against Defendant Keystone Health ("Keystone" or "Defendant") and complains and alleges upon personal knowledge as to themselves and upon information and belief as to all other matters.

INTRODUCTION

1. Plaintiffs bring this class action against Keystone for its failure to secure and safeguard personally identifiable information ("PII") and personal health information ("PHI") (collectively, "Personal Information") for approximately 235,237 patients of or other persons affiliated with Keystone.

2. Defendant is Pennsylvania-based entity comprised of primary care providers serving the greater Franklin County Pennsylvania region. Keystone

describes itself as a "full-service, family-centered, primary care facility providing quality, affordable, accessible health care."

3. As a condition of receiving healthcare services, Keystone's clients and their patients are required to provide and entrust Keystone with sensitive and private information, including PII and PHI. The Personal Information that Keystone collects and maintains includes names, addresses, healthcare member IDs, and other information provided during health assessments.

4. On or around August 19, 2022, Keystone identified an incident that temporarily disrupted its computer systems.

5. Keystone's investigation revealed that an unauthorized party had accessed files within its system between July 28, 2022 and August 19, 2022 (the "Data Breach").

6. The impacted files contained patient information, including names, Social Security numbers, and clinical information.

7. Keystone did not announce the Data Breach publicly until on or around October 14, 2022, and did not begin sending out Data Breach notification letters to patients until around that time.

8. Keystone's notice on its website provides scant detail about the Data Breach and the steps that Keystone is taking to address it. The notice merely states that Keystone "identified an incident that temporarily disrupted our computer

systems" and that it "worked with a third-party cybersecurity firm to determine what happened." It further reports that its "investigation found that an unauthorized party accessed files within our system between July 28, 2022 and August 19, 2022" and that "[s]ome of those files contained patient information, including names, Social Security numbers, and clinical information." Keystone stated that it would be mailing letters to affected patients and offering credit monitoring services "to those who are eligible." It also vaguely asserted that it was "implementing new network security measures and providing additional training to [its] employees" to "help prevent something like this from happening again."[1]

9. Keystone's notice did not disclose how it discovered the encrypted files on its computer systems were impacted, the means and mechanism of the cyberattack, the reason for the two month delay in notifying Plaintiffs and the Class of the Data Breach, how Keystone determined that the PII/PHI had been "accessed" by the unauthorized actor, and, importantly, what steps Keystone took following the Data Breach to secure its systems and prevent future cyberattacks.

10. The Data Breach was a direct result of Keystone's failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect patients' Personal Information from the foreseeable threat of a cyberattack.

[1] Keystone Notice of Security Incident, available: https://keystonehealth.org/wp-content/notice_pdf/notice_of_security_incident.pdf (last accessed Oct. 18, 2022).

11. By being entrusted with Plaintiffs' and Class Members' Personal Information for its own pecuniary benefit, Keystone assumed a duty to Plaintiffs and Class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard Plaintiffs' and Class members' Personal Information against unauthorized access and disclosure. Keystone also had a duty to adequately safeguard this Personal Information under controlling Pennsylvania case law, as well as pursuant to industry standards and duties imposed by statutes, including HIPAA regulations and Section 5 of the Federal Trade Commission Act ("FTC Act"). Keystone breached those duties by, among other things, failing to implement and maintain reasonable security procedures and practices to protect patients' Keystone from unauthorized access and disclosure.

12. As a result of Keystone's inadequate security and breach of its duties and obligations, the Data Breach occurred, and Plaintiffs and over 235,000 Class Members suffered injury and ascertainable losses in the form of out-of-pocket expenses, loss of value of their time reasonably incurred to remedy or mitigate the effects of the attack, the diminution in value of their personal information from its exposure, and the present and imminent thread of fraud and identity theft. This action seeks to remedy these failings and their consequences.

13. The injury to Plaintiffs and Class Members was compounded by the fact that Keystone did not notify patients that their Personal Information was subject

to unauthorized access and exfiltration until October 14, nearly two months after the Data Breach was discovered. Keystone's failure to timely notify the victims of its Data Breach meant that Plaintiffs and Class Members were unable to immediately take affirmative measures to prevent or mitigate the resulting harm.

14. Despite having been accessed and exfiltrated by unauthorized criminal actors, Plaintiffs' and Class Members' sensitive and confidential Personal Information still remains in the possession of Keystone. Absent additional safeguards and independent review and oversight, the information remains vulnerable to further cyberattacks and theft.

15. Keystone disregarded the rights of Plaintiffs and Class Members by, *inter alia*, failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard patient Personal Information; failing to take standard and reasonably available steps to prevent the Data Breach; failing to properly train its staff and employees on proper security measures; and failing to provide Plaintiffs and Class Members prompt and adequate notice of the Data Breach.

16. In addition, Keystone and its employees failed to properly monitor the computer network and systems that housed the Personal Information. Had Keystone

properly monitored these electronic systems, it would have discovered the intrusion sooner or prevented it altogether.

17. The security of Plaintiffs' and Class Members' identities is now at risk because of Keystone's wrongful conduct as the Personal Information that Keystone collected and maintained is now in the hands of data thieves. This present risk will continue for the course of their lives.

18. Armed with the Personal Information accessed in the Data Breach, data thieves can commit a wide range of crimes including, for example, opening new financial accounts in Class Members' names, taking out loans in their names, using Class Members' identities to obtain government benefits, filing fraudulent tax returns using their information, obtaining driver's licenses in Class Members' names, and giving false information to police during an arrest.

19. As a result of the Data Breach, Plaintiffs and Class Members have been exposed to a present and imminent risk of fraud and identity theft. Among other measures, Plaintiffs and Class Members must now and in the future closely monitor their financial accounts and medical records to guard against identity theft. Further, Plaintiffs and Class Members will incur out-of-pocket costs to purchase credit monitoring and identity theft protection and insurance services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

20. Plaintiffs and Class Members will also be forced to expend additional time to review credit reports and monitor their financial accounts and medical records for fraud or identity theft. And because the exposed information includes Social Security numbers and other immutable personal details, the risk of identity theft and fraud will persist throughout their lives.

21. Plaintiffs bring this action on behalf of themselves and individuals in the United States whose Personal Information was exposed as a result of the Data Breach, which Keystone learned of on or about August 19, 2022 and first publicly acknowledged on or about October 14, 2022. Plaintiffs and Class Members seek to hold Keystone responsible for the harms resulting from the massive and preventable disclosure of such sensitive and personal information. Plaintiffs seek to remedy the harms resulting from the Data Breach on behalf of themselves and all similarly situated individuals whose Personal Information was accessed and exfiltrated during the Data Breach.

22. Plaintiffs, on behalf of themselves and all other Class Members, bring claims for negligence, negligence per se, breach of fiduciary duty, breach of implied contract, unjust enrichment, and for declaratory and injunctive relief. To remedy these violations of law, Plaintiffs and class members thus seek actual damages, statutory damages, restitution, and injunctive and declaratory relief (including significant improvements to Keystone's data security protocols and employee

training practices), reasonable attorneys' fees, costs, and expenses incurred in bringing this action, and all other remedies this Court deems just and proper.

PARTIES

Plaintiffs

Plaintiff Breneman

23. Plaintiff Kylie Breneman is a resident and citizen of the Commonwealth of Pennsylvania.

24. Plaintiff Breneman provided her PII/PHI to Keystone in connection with receiving health care services from Keystone.

25. On or about October 17, 2022, Plaintiff Breneman received a letter from Keystone notifying her that her PII/PHI may have been exposed in the Data Breach.

26. Had Plaintiff Breneman known that Keystone does not adequately protect PII/PHI, she would not have used Keystone's services and agreed to provide Keystone with her PII/PHI.

27. As a result of Keystone Medical's failure to adequately safeguard Plaintiff Breneman's information, she has been injured.

Plaintiff Arroyo-Ryan

28. Plaintiff Brandy Arroyo-Ryan is a resident and citizen of the Commonwealth of Pennsylvania.

29. Plaintiff Arroyo-Ryan is a patient of WellSpan OB/GYN in Waynesboro, PA, which upon information and belief, shares a record keeping system operated by Keystone.

30. Plaintiff Arroyo-Ryan provided her personal and health information to WellSpan OB/GYN in order to receive medical care. Keystone received Plaintiff's personal and health information in connection with providing healthcare services. In maintaining her Private Information, Keystone expressly and impliedly promised to safeguard Plaintiff Arroyo-Ryan's Private Information. Keystone, however, did not take proper care of Plaintiff Arroyo-Ryan's Private Information, leading to its exposure to and exfiltration by cybercriminals as a direct result of Keystone Medical's inadequate security measures.

31. Plaintiff Arroyo-Ryan received a letter dated October 14, 2022 from Keystone concerning the Data Breach. The letter stated that an unauthorized party gained access to Plaintiff's personal information from data stored on Keystone's systems. The notice stated that the compromised information that was present on the impacted files included Plaintiff's name, social security number, and other medical information.

32. Plaintiff Arroyo-Ryan paid for medical services with the expectation that WellSpan and its partners, like Keystone, would keep her information secure and inaccessible from unauthorized parties.

33. Plaintiff Arroyo-Ryan and Class Members have faced and will continue to face a certainly impending and substantial risk of injury as a result of Keystone's ineffective data security measures. Some harms may not materialize for years after the Data Breach, rendering Keystone's notice letter woefully inadequate to address and prevent the fraud that has occurred and will continue to occur through the misuse of Class Members' information.

34. Plaintiff Arroyo-Ryan greatly values her privacy, especially while receiving medical services. She would not have obtained medical services from WellSpan/Keystone, or paid the amount she did to receive medical services, had she known that her healthcare provider's marketing service provider would negligently fail to adequately protect her Private Information.

35. Plaintiff Arroyo-Ryan suffers stress and anxiety as a result of the Data Breach and from the loss of her privacy.

36. Plaintiff Arroyo-Ryan also suffered injury in the form of damage to and diminution in the value of her confidential personal information—a form of property that Plaintiff Arroyo-Ryan entrusted to Keystone, which was compromised as a result of the Data Breach it failed to prevent.

37. Plaintiff Arroyo-Ryan suffers a present injury from the existing and continuing risk of fraud, identity theft, and misuse resulting from his/her/their personal information—especially her name, address and sensitive medical

information—being placed in the hands of unauthorized third parties. Plaintiff Arroyo-Ryan has a continuing interest in ensuring that her personal information is protected and safeguarded from future breaches.

Defendant

38. Defendant Keystone Health is a 501(c) Pennsylvania-based healthcare provider that is the only federally-qualified Community Health Center serving Franklin County, Pennsylvania. Its principal place of business is located at 111 Chambers Hill Drive, Chambersburg, PA 17201.

JURISDICTION AND VENUE

39. This Court has jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2)(A), as modified by the Class Action Fairness Act of 2005, because at least one member of the Class is a citizen of a different state than Defendant, there are more than 100 members of the Class, and the aggregate amount in controversy exceeds $5,000,000 exclusive of interests and costs.

40. This Court has personal jurisdiction over Keystone because Keystone maintains its principal place of business in Pennsylvania and conducts substantial business in Pennsylvania and in this district through its principal place of business; engaged in the conduct at issue herein from and within this District; and otherwise has substantial contacts with this District and purposely availed itself of the Courts in this District.

41. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b)(1) and (2) because Keystone resides in this district, and this district is where a substantial part of the acts, omissions, and events giving rise to Plaintiffs' claims occurred.

FACTUAL ALLEGATIONS

A. Overview of Keystone Health

42. Keystone is a health center that provides healthcare services through fifteen locations throughout Pennsylvania. Keystone is supported by the Health Resources and Services Administration (HRSA) of the U.S. Department of Health and Human Services (HHS).

43. In the regular course of its business, Keystone collects and maintains the PII/PHI of patients, former patients, and other persons to whom it is currently providing or previously provided health-related or other services.

44. As a regular part of its business, Keystone requires patients to provide personal information before it provides them services. That information includes, *inter alia*, names, addresses, dates of birth, health insurance information, and Social Security numbers. Keystone stores this information digitally.

45. As a HIPAA covered business entity (*see infra*), Keystone is required to implement adequate safeguards to prevent unauthorized use or disclosure of Personal Information, including by implementing requirements of the HIPAA

Security Rule[2] and to report any unauthorized use or disclosure of Personal Information, including incidents that constitute breaches of unsecured protected health information as in the case of the Data Breach complained of herein.

46. In their Privacy Notice, Keystone states that it is "required by law to maintain the privacy and security of your protected health information" and that "We will let you know promptly if a breach occurs that may have compromised the privacy and security of your information."[3]

47. Yet, Keystone waited nearly two (2) months after discovering the data breach to notify its patients that their PII/PHI had been compromised.

48. Plaintiffs and Class members are, or were, patients of Keystone or received health-related or other services from Keystone, or otherwise are affiliated or transacted with Keystone, and entrusted Keystone with their PII/PHI.

B. Keystone Is a HIPAA Covered Business associate

49. Keystone is a healthcare provider that provides healthcare services through fifteen locations throughout Pennsylvania. Keystone is supported by the

[2] The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information. *See* 45 C.F.R. Part 160 and Part 164, Subparts A and C.

[3] Keystone Health, *Notice of Privacy Practices*, KEYSTONEHEALTH.ORG, https://keystonehealth.org/wp-content/uploads/2019/01/notice-of-privacy-practices-January-2019.pdf (last visited Oct. 18, 2022).

Health Resources and Services Administration (HRSA) of the U.S. Department of Health and Human Services (HHS).

50. In the regular course of its business, Keystone collects and maintains the Personal Information of patients, former patients, and other persons through its healthcare providers.

51. Keystone is a HIPAA covered business associate that provides healthcare services to patients. As a regular and necessary part of its business Keystone collects and custodies the highly sensitive Patient Information of its patients. Keystone is required under federal and state law to maintain the strictest confidentiality of the patient's Personal Information that it requires, receives, and collects, and Keystone is further required to maintain sufficient safeguards to protect that Personal Information from being accessed by unauthorized third parties.

52. As a HIPAA covered business entity, Keystone is required to implement adequate safeguards to prevent unauthorized use or disclosure of Personal Information, including by implementing requirements of the HIPAA Security Rule[4] and to report any unauthorized use or disclosure of Personal

[4] The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information. *See* 45 C.F.R. Part 160 and Part 164, Subparts A and C.

Information, including incidents that constitute breaches of unsecured protected health information as in the case of the Data Breach complained of herein.

53. As a condition of receiving Keystone's services, Keystone requires that patients, including Plaintiffs and Class Members, entrust it with highly sensitive personal information. Due to the nature of Keystone's business of providing healthcare services, Keystone would be unable to engage in its regular business activities without collecting and aggregating Personal Information that it knows and understands to be sensitive and confidential.

54. Keystone recognizes its responsibility, as "required by law," "to maintain the privacy and security of [patient's] protected health information." Its Notice of Privacy Practices brochure states that Keystone "will let [patients] know promptly if a breach occurs that may have comprised the privacy or security of [patients'] information."[5]

55. Plaintiffs and Class members are or were patients whose medical records were maintained by, or who received health-related or other services from, Keystone and directly or indirectly entrusted Keystone with their Personal Information. Plaintiffs and Class members reasonably expected that Keystone would

[5] *See* Keystone Health, Notice of Privacy Practices, available at: notice-of-privacy-practices-January-2019.pdf (keystonehealth.org) (last accessed Oct. 18, 2022).

safeguard their highly sensitive information and keep their Personal Information confidential.

C. The Data Breach Compromised Plaintiffs' and Class Members' PII/PHI

56. On or about August 19, 2022, according to the notice Keystone posted to its website, Keystone identified an incident that temporarily disrupted its computer systems. It launched an investigation with the assistance of third-party cybersecurity firm to determine the nature and scope of the activity.

57. Keystone's investigation determined that an unauthorized party accessed files within its systems between July 28, 2022 and August 19, 2022.

58. Keystone did not publicly announce the Data Breach until two months later. It provided a summary of the Data Breach on its website on or around October 14, 2022. It stated that it was mailing letters to affected patients. The press release Keystone posted on its website states that the unauthorized party accessed files within its system that "contained patient information, including names, Social Security numbers, and clinical information."

59. Keystone's press release also vaguely describes the measures it took following its discovery of the Data Breach, stating only that:

> To help prevent something like this from happening again, we are implementing new network security measures and providing additional training to our employees.[6]

60. Keystone's notice omits pertinent information including how criminals gained access to the encrypted files on its systems, what computer systems were impacted, the means and mechanisms of the cyberattack, the reason for the two month delay in notifying Plaintiffs and Class Members of the Data Breach, how it determined that the Personal Information had been "accessed," and of particular importance to Plaintiffs and Class Members, what actual steps Keystone took following the Data Breach to secure its systems and train its employees to prevent further cyberattacks.

61. Based on Keystone's acknowledgment that Personal Information was "accessed" by an unauthorized party, it is evident that unauthorized criminal actors did in fact access Keystone's network and exfiltrate Plaintiffs' and Class Members' Personal Information in an attack designed to acquire that sensitive, confidential, and valuable information.

62. The Personal Information contained in the files accessed by cybercriminals appears not to have been encrypted because if properly encrypted,

[6] *See* Keystone Health, Notice of Security Incident, available at https://keystonehealth.org/wp-content/notice_pdf/notice_of_security_incident.pdf (last accessed Oct. 19, 2022).

the attackers would have acquired unintelligible data and would not have "accessed" Plaintiffs' and Class Members' Personal Information.

63. The company said it determined that the compromised systems contained Personal Information provided by its patients, including names, Social Security numbers and clinical information. It does not specify what type of "clinical information" was compromised.

64. Keystone provides healthcare services at fifteen different locations. It did not confirm whether some or all of its locations were impacted by the Data Breach. The Data Breach reportedly impacted the protected health information of 235,237 individuals.[7]

65. As a HIPAA associated business entity that collects, creates, and maintains significant volumes of Private Information, the targeted attack was a foreseeable risk of which KEYSTONE was aware and knew it had a duty to guard against.

66. The targeted attack was expressly designed to gain access to and exfiltrate private and confidential data, including (among other things) the Personal Information of patients, like Plaintiffs and Class Members.

[7] Jill McKeon, *Keystone Health Data Breach Impacts PHI of 235K Individuals*, Health IT Security (Oct. 17, 2022), available at: https://healthitsecurity.com/news/keystone-health-data-breach-impacts-phi-of-235k-individuals (last accessed Oct. 18, 2022).

67. Despite detecting the Data Breach on or around August 19, 2022, Keystone waited nearly two months following the completion of its investigation to notify the impacted individuals of the Data Breach and of the need for them to protect themselves against fraud and identity theft. Keystone was, of course, too late in the discovery and notification of the Data Breach.

68. Due to Keystone's inadequate security measures and its delayed notice to victims, Plaintiffs and Class Members now face a present, immediate, and ongoing risk of fraud and identity theft and must deal with that threat forever.

69. Keystone had obligations created by HIPAA, contract, industry standards and common law made to Plaintiffs and Class Members to keep their Personal Information confidential and to protect it from unauthorized access and disclosure.

70. Plaintiffs and Class Members entrusted their Personal Information to Keystone's clients with the reasonable expectation and mutual understanding that Keystone or anyone who used their Personal Information in conjunction with the healthcare services they received would comply with obligations to keep such information confidential and secure from unauthorized access after it received such information.

71. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Keystone assumed legal and equitable

duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Personal Information from unauthorized disclosure.

72. Plaintiffs and the Class Members have taken reasonable steps to maintain the confidentiality of their personal information. Plaintiffs and Class Members would not have allowed Keystone or anyone in Keystone's position to receive their PII/PHI had they known that Keystone would fail to implement industry standard protections for that sensitive information.

73. As a result of Keystone's negligent and wrongful conduct, Plaintiffs' and Class Members' highly confidential and sensitive Personal Information was left exposed to cybercriminals.

D. Defendant Was Obligated Under HIPAA to Safeguard the Personal Information

71. Keystone is a covered business associate under HIPAA (45 C.F.R. § 160.102) and is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

72. Keystone is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information

Technology Act ("HITECH").[8] *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

73. HIPAA's Privacy Rule or *Standards for Privacy of Individually Identifiable Health Information* establishes national standards for the protection of health information.

74. HIPAA's Privacy Rule or *Security Standards for the Protection of Electronic Protected Health Information* establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

75. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

76. "Electronic protected health information" is "individually identifiable health information … that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

77. HIPAA's Security Rule requires Keystone to do the following:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

[8] HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by its workforce.

78. HIPAA also requires Keystone to "review and modify the security measures implemented … as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e). Additionally, Keystone is required under HIPAA to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

79. HIPAA and HITECH also obligated Keystone to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. §17902.

80. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires Keystone to provide notice of the Data Breach to each affected individual

"without unreasonable delay and in no case later than 60 days following discovery of the breach."[9]

81. HIPAA requires a covered entity to have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).

82. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

83. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis

[9] Breach Notification Rule, U.S. Dep't of Health & Human Services, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (emphasis added).

requirements of the Security Rule." US Department of Health & Human Services, Security Rule Guidance Material.[10] The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says "represent the industry standard for good business practices with respect to standards for securing e-PHI." US Department of Health & Human Services, Guidance on Risk Analysis.[11]

E. Keystone Failed to Follow FTC Guidelines

84. Keystone was also prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (the "FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

85. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices.

86. According to the FTC, the need for data security should be factored into all business decision-making.

---

[10] http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html.

[11] https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html.

87. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses.

88. The guidelines note that businesses should protect the personal patient information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

89. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

90. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

91. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect patient data, treating the failure to employ

reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

92. Keystone failed to properly implement basic data security practices.

93. Keystone's failure to employ reasonable and appropriate measures to protect against unauthorized access to patients' and plan members Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

94. Keystone was at all times fully aware of its obligation to protect the Private Information of the patients and plan members about whom it stored Private Information. Keystone was also aware of the significant repercussions that would result from its failure to do so.

F. Keystone Failed to Comply with Industry Standards

95. As described above, experts studying cyber security routinely identify healthcare providers and their business associates as being particularly vulnerable to cyberattacks because of the value of the PII and PHI which they collect and maintain.

96. Several best practices have been identified that at a minimum should be implemented by HIPAA covered business entities like Keystone, including but not limited to: educating all employees; strong passwords; multi-layer security,

including firewalls, anti-virus, and anti- malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

97. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

98. Keystone failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

99. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and Keystone failed to comply with these accepted standards, thereby opening the door to cybercriminals and causing the Data Breach.

G. Keystone Owed Plaintiffs and Class Members a Duty to Safeguard Their Personal Information

100. In addition to its obligations under federal and state laws, Keystone owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Keystone owed a duty to Plaintiffs and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the Private Information of Class Members.

101. Keystone owed a duty to Plaintiffs and Class Members to create and implement reasonable data security practices and procedures to protect the Private Information in its possession, including adequately training its employees and others who accessed Private Information within its computer systems on how to adequately protect Private Information.

102. Keystone owed a duty to Plaintiffs and Class Members to implement processes that would detect a compromise of Private Information in a timely manner.

103. Keystone owed a duty to Plaintiffs and Class Members to act upon data security warnings and alerts in a timely fashion.

104. Keystone owed a duty to Plaintiffs and Class Members to disclose in a timely and accurate manner when and how the Data Breach occurred.

105. Keystone owed a duty of care to Plaintiffs and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

H. Keystone Knew That Criminals Target PII/PHI

106. Keystone's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the healthcare industry and other industries holding significant amounts of PII and PHI preceding the date of the breach.

107. At all relevant times, Keystone knew, or should have known, its patients', Plaintiffs', and all other Class members' PII/PHI was a target for malicious actors. Despite such knowledge, Keystone failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiffs' and Class members' Private Information from cyber-attacks that Keystone should have anticipated and guarded against.

108. The targeted attack was expressly designed to gain access to and exfiltrate private and confidential data, including (among other things) the Private Information of patients and/or plan members, like Plaintiffs and Class Members.

109. Cyber criminals seek out PHI at a greater rate than other sources of personal information. In a 2022 report, the healthcare compliance company Proetus found that there were 905 medical data breaches in 2021, leaving over 50 million

patient records exposed for 700 of the 2021 incidents. This is an increase from the 758 medical data breaches that Protenus compiled in 2020.[12]

110. The healthcare sector suffered about 337 breaches in the first half of 2022 alone, according to Fortified Health Security's mid-year report released in July. The percentage of healthcare breaches attributed to malicious activity rose more than 5 percentage points in the first six months of 2022 to account for nearly 80 percent of all reported incidents.[13]

111. Further, a 2022 report released by IBM Security states that for 12 consecutive years the healthcare industry has had the highest average cost of a data breach and as of 2022 healthcare data breach costs have hit a new record high.[14]

112. PII/PHI is a valuable property right.[15] The value of PII/PHI as a

---

[12] *2022 Breach Barometer*, PROTENUS, https://www.protenus.com/breach-barometer-report (last visited Aug. 2, 2022).

[13] Jill McKeon, *Health Sector Suffered 337 Healthcare Data Breaches in First Half of Year*, Cybersecurity News (July 19, 2022), available: https://healthitsecurity.com/news/health-sector-suffered-337-healthcare-data-breaches-in-first-half-of-year (last visited October 5, 2022).

[14] *Cost of a Data Breach Report 2022*, IBM Security, available: https://www.ibm.com/downloads/cas/3R8N1DZJ.

[15] *See* Marc van Lieshout, *The Value of Personal Data*, 457 IFIP ADVANCES IN INFORMATION AND COMMUNICATION TECHNOLOGY 26 (May 2015), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible...").

commodity is measurable.[16] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[17] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[18] It is so valuable to identity thieves that once PII/PHI has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

113. As a result of its real value and the recent large-scale data breaches, identity thieves and cyber criminals have openly posted credit card numbers, Social Security numbers, PII/PHI, and other sensitive information directly on various Internet websites, making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims.

---

[16] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE (Apr. 28, 2014), http://www.medscape.com/viewarticle/824192.

[17] *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD 4 (Apr. 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

[18] *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, INTERACTIVE ADVERTISING BUREAU (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

114. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[19] A cybercriminal who steals a person's PHI can end up with as many as "seven to 10 personal identifying characteristics of an individual."[20] A study by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[21]

115. All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, SSNs, and bank account information, complete with account and routing numbers, can fetch up to $1,200 to $1,300 each on the black market.[22] According to a report released by the Federal Bureau of Investigation's ("FBI") Cyber Division, criminals

[19] *See* Andrew Steger, *What Happens to Stolen Healthcare Data?*, HEALTHTECH MAGAZINE (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating "Health information is a treasure trove for criminals.").

[20] *Id.*

[21] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010, 5:00 AM), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims.

[22] Adam Greenberg, *Health insurance credentials fetch high prices in the online black market*, SC MAGAZINE (July 16, 2013), https://www.scmagazine.com/news/breach/health-insurance-credentials-fetch-high-prices-in-the-online-black-market.

can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.[23]

116. Criminals can use stolen PII/PHI to extort a financial payment by "leveraging details specific to a disease or terminal illness."[24] Quoting Carbon Black's Chief Cybersecurity Officer, one recent article explained: "Traditional criminals understand the power of coercion and extortion . . . . By having healthcare information—specifically, regarding a sexually transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do."[25]

117. Consumers place a high value on the privacy of that data. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[26]

---

[23] *See Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain*, FBI CYBER DIVISION (Apr. 8, 2014), https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf.

[24] *See* n.8, *supra*.

[25] *Id.*

[26] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011), https://www.jstor.org/stable/23015560?seq=1.

118. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII/PHI has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

119. Indeed, cyberattacks against the healthcare industry have been common for over ten years with the Federal Bureau of Investigation ("FBI") warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime."[27]

120. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals… because they often have lesser IT defenses and a high incentive to regain access to their data quickly.[28]

---

[27] Gordon M. Snow, *Statement before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit*, FBI (Sept. 14, 2011), https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector.

[28] *FBI, Secret Service Warn of Targeted*, Law360 (Nov. 18, 2019), https://www.law360. arn-of-targeted-ransomware (last visited July 2, 2021).

121. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[29]

122. Keystone was on notice that the FBI has recently been concerned about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[30]

123. The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting their patients' confidential information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.[31]

---

[29] *See* Maria Henriquez, *Iowa City Hospital Suffers Phishing Attack*, *Security Magazine* (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack

[30] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, REUTERS (Aug. 2014), https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820.

[31] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, AM. MED. ASS'N (Oct. 4, 2019), https://www.ama-assn.org/practice-

124. As implied by the above AMA quote, stolen Private Information can be used to interrupt important medical services. This is an imminent and certainly impending risk for Plaintiffs and Class Members.

125. Keystone was on notice that the federal government has been concerned about healthcare company data encryption practices. Keystone knew its employees accessed and utilized protected health information in the regular course of their duties, yet it appears that information was not encrypted.

126. The Office for Civil Rights ("OCR") urges the use of encryption of data containing sensitive personal information. As long ago as 2014, the Department fined two healthcare companies approximately two million dollars for failing to encrypt laptops containing sensitive personal information. In announcing the fines, Susan McAndrew, OCR's deputy director of health information privacy, stated "[o]ur message to these organizations is simple: encryption is your best defense against these incidents."[32]

management/sustainability/cybersecurity-ransomeware-attacks-shut-down-clinics-hospitals.

[32] "Stolen Laptops Lead to Important HIPAA Settlements," U.S. Dep't of Health and Human Services (Apr. 22, 2014), available at https://wayback.archive-it.org/3926/20170127085330/https://www.hhs.gov/about/news/2014/04/22/stolen-laptops-lead-to-important-hipaa-settlements.html.

127. As a HIPAA covered business associate, Keystone should have known about its data security vulnerabilities and implemented enhanced and adequate protection, particularly given the nature of the PII/PHI stored in its unprotected files.

I. Theft of PII/PHI Has Grave and Lasting Consequences for Victims

128. Theft of PII/PHI is serious. The Federal Trade Commission ("FTC") warns consumers that identity thieves use PII/PHI to exhaust financial accounts, receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.[33]

129. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[34] According to Experian, one of the largest credit reporting companies in the world, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan, change a billing address so the victim no longer receives bills, open

[33] *See What to Know About Identity Theft*, FEDERAL TRADE COMMISSION CONSUMER ADVICE, https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last visited Aug. 2, 2022).

[34] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 12 C.F.R. § 1022.3(h). The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 12 C.F.R. § 1022.3(g).

new utilities, obtain a mobile phone, open a bank account and write bad checks, use a debit card number to withdraw funds, obtain a new driver's license or ID, and/or use the victim's information in the event of arrest or court action.[35]

130. With access to an individual's PII/PHI, criminals can do more than just empty a victim's bank account—they can also commit all manner of fraud, including: obtaining a driver's license or official identification card in the victim's name but with the thief's picture, using the victim's name and SSN to obtain government benefits, or filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house, or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[36]

131. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States. For example, with the Private Information stolen in the Data Breach, which includes Social Security numbers, identity thieves can open financial accounts, commit medical fraud, apply for credit, file fraudulent tax

[35] Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself?*, EXPERIAN (Sept. 1, 2017), https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

[36] *See Warning Signs of Identity Theft*, FEDERAL TRADE COMMISSION, https://www.identitytheft.gov/
Warning-Signs-of-Identity-Theft (last visited Aug. 2, 2022).

returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft. These criminal activities have and will result in devastating financial and personal losses to Plaintiffs and Class Members.

132. PII/PHI is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it and trade the information on dark web black-markets for years.

133. For example, it is believed that certain highly sensitive personal information compromised in the 2017 Experian data breach was being used, three years later, by identity thieves to apply for COVID-19-related unemployment benefits.

134. The Personal Information exposed in this Data Breach is valuable to identity thieves for use in the kinds of criminal activity described herein. These risks are both certainly impending and substantial. As the FTC has reported, if cyber thieves get access to a person's highly sensitive information, they will use it.[37]

[37] Ari Lazarus, *How fast will identity thieves use stolen info?*, FED. TRADE COMM'N (May 24, 2017), https://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-info.

135. Cyber criminals may not use the information right away. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[38]

136. For instance, with a stolen Social Security number, which is only one subset of the Private Information compromised in the Data Breach, someone can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.[39]

137. Identity thieves can use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's

[38] *Data Breaches Are Frequent*, *supra* note 11.
[39] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 2, 2017, https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/.

personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

138. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."

139. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.[40]

140. Theft of Social Security numbers also creates a particularly alarming situation for victims because those numbers cannot easily be replaced. In order to obtain a new number, a breach victim has to demonstrate ongoing harm from misuse of her SSN, and a new SSN will not be provided until after the victim has suffered the harm.

141. Due to the highly sensitive nature of Social Security numbers, theft of Social Security numbers in combination with other PII (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. TIME quotes

[40] *2021 Consumer Aftermath Report: How Identity Crimes Impact Victims, their Families, Friends, and Workplaces*, IDENTITY THEFT RESOURCE CENTER (2021), https://www.idtheftcenter.org/identity-theft-aftermath-study/ (last visited Aug. 2, 2022).

data security researcher Tom Stickley, who is employed by companies to find flaws in their computer systems, as stating, "If I have your name and your Social Security number and you haven't gotten a credit freeze yet, you're easy pickings."[41]

142. Theft of PII is even more serious when it includes theft of PHI. Medical identity theft is one of the most common, most expensive, and most difficult-to-prevent forms of identity theft. According to Kaiser Health News, "medical-related identity theft accounted for 43 percent of all identity thefts reported in the United States in 2013," which is more than identity thefts involving banking and finance, the government and the military, or education.[42] "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[43]

143. Data breaches involving medical information "typically leave[] a trail of falsified information in medical records that can plague victims' medical and

[41] Patrick Lucas Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (Aug. 5, 2019, 3:39 PM), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.
[42] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, https://khn.org/news/rise-of-indentity-theft/
[43] *Id.*

financial lives for years."[44] It "is also more difficult to detect, taking almost twice as long as normal identity theft."[45] In warning consumers on the dangers of medical identity theft, the FTC states that an identity thief may use PII/PHI "to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care." [46] The FTC also warns, "If the thief's health information is mixed with yours, it could affect the medical care you're able to get or the health insurance benefits you're able to use. It could also hurt your credit."[47]

144. A report published by the World Privacy Forum and presented at the US FTC Workshop on Informational Injury describes what medical identity theft victims may experience:

- Changes to their health care records, most often the addition of falsified information, through improper billing activity or activity by imposters. These changes can affect the healthcare a person receives if the errors are not caught and corrected.
- Significant bills for medical goods and services not sought nor received.
- Issues with insurance, co-pays, and insurance caps.
- Long-term credit problems based on problems with debt collectors reporting debt due to identity theft.

[44] Pam Dixon and John Emerson, *The Geography of Medical Identity Theft*, WORLD PRIVACY FORUM 6 (Dec. 12, 2017), https://www.worldprivacyforum.org/2017/12/new-report-the-geography-of-medical-identity-theft/.
[45] *See* n.20, *supra*.
[46] *See* n.30, *supra*.
[47] *Id.*

- Serious life consequences resulting from the crime; for example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed from them due to medical activities of the imposter; victims have been denied jobs due to incorrect information placed in their health files due to the crime.

- As a result of improper and/or fraudulent medical debt reporting, victims may not qualify for mortgage or other loans and may experience other financial impacts.

- Phantom medical debt collection based on medical billing or other identity information.

- Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own.[48]

145. There may also be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. Fraud and identity theft resulting from the Data Breach may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

[48] *See* n.41, *supra*.

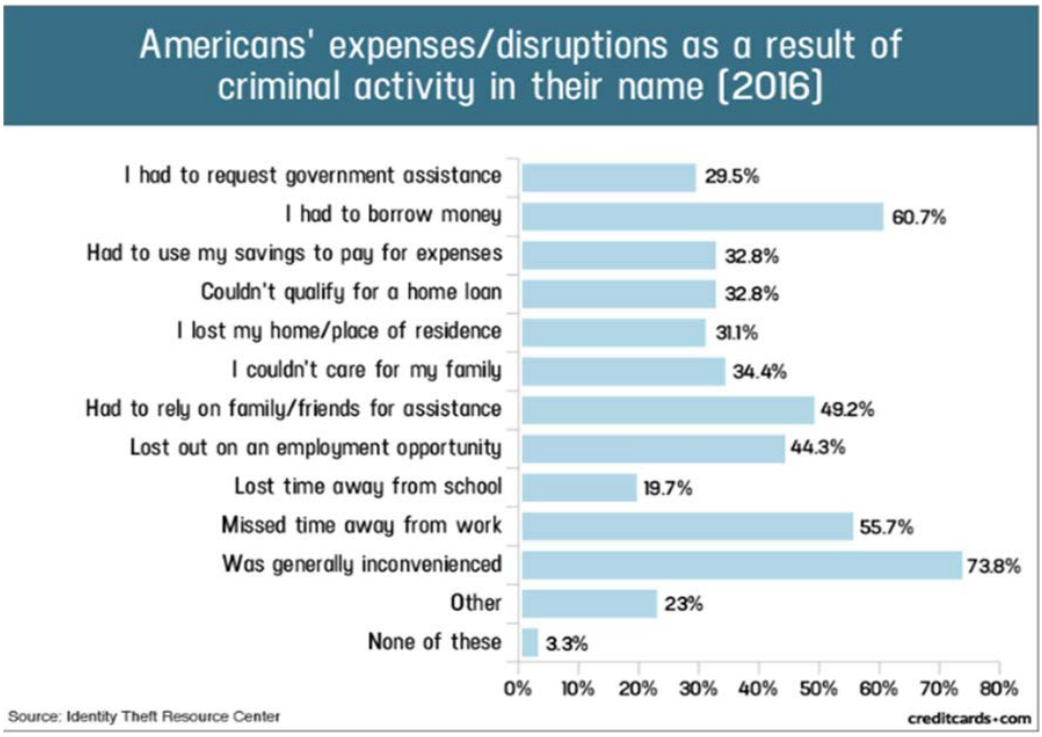
146. For example, on average it takes approximately three months for consumers to discover their identity has been stolen and used, and it takes some individuals up to three years to learn that information.[49]

147. It is within this context that Plaintiffs and all other Class members must now live with the knowledge that their PII/PHI is forever in cyberspace and was taken by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black market.

148. A study by the Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information.[50]

[49] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 JOURNAL OF SYSTEMICS, CYBERNETICS AND INFORMATICS 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

[50] *See* Jason Steele, Credit Card and ID Theft Statistics, CreditCards.com (Oct. 23, 2020) https:// www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php.



149. Victims of the Data Breach, like Plaintiffs and Class Members, must spend many hours and large amounts of money protecting themselves from the current and future negative impacts to their privacy and credit because of the Data Breach.[51]

150. As a direct and proximate result of the Data Breach, Plaintiffs and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. Plaintiffs and Class Members must now take the time and effort (and spend the money) to mitigate the actual and potential impact of the Data Breach on their everyday lives, including purchasing identity

[51] "Guide for Assisting Identity Theft Victims," Federal Trade Commission, 4 (Sept. 2013), http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf.

theft and credit monitoring services every year for the rest of their lives, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions and healthcare providers, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, credit reports, and health insurance account information for unauthorized activity for years to come.

151. Plaintiffs and Class Members have suffered or will suffer actual harms for which they are entitled to compensation, including but not limited to the following:

a. Trespass, damage to, and theft of their personal property, including Private Information;

b. Improper disclosure of their Private Information;

c. The imminent and certainly impending injury flowing from actual and potential future fraud and identity theft posed by their Private Information being in the hands of criminals and having already been misused;

d. The imminent and certainly impending risk of having their confidential medical information used against them by spam callers to defraud them;

e. Damages flowing from Defendant's untimely and inadequate notification of the Data Breach;

f. Loss of privacy suffered as a result of the Data Breach;

g. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the data breach;

h. Ascertainable losses in the form of deprivation of the value of patients' personal information for which there is a well-established and quantifiable national and international market;

i. The loss of use of and access to their credit, accounts, and/or funds;

j. Damage to their credit due to fraudulent use of their Private Information; and

k. Increased cost of borrowing, insurance, deposits, and other items which are adversely affected by a reduced credit score.

152. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which remains in the possession of Defendant, is protected from further public disclosure by the implementation of better employee training and industry standard and statutorily compliant security measures and safeguards. Defendant has shown itself to be wholly incapable of protecting Plaintiffs' and Class Members' Private Information.

153. Because of the value of its collected and stored data, the medical industry has experienced disproportionally higher numbers of data theft events than

other industries. For this reason, Defendant knew or should have known about these dangers and strengthened its data security accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

J. The Data Breach Was Foreseeable and Preventable

154. Data disclosures and data breaches are preventable.[52] As Lucy Thompson wrote in the Data Breach and Encryption Handbook, "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[53] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[54]

155. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures … Appropriate information security controls, including encryption, must be

[52] Lucy L. Thompson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).
[53] *Id.* at 17.
[54] *Id.* at 28.

implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[55]

156. Plaintiffs and Class Members entrusted their Private Information to Keystone as a condition of receiving healthcare related services. Plaintiffs and Class Members understood and expected that Keystone or anyone in Keystone's position would safeguard their Private Information against cyberattacks, delete or destroy Private Information that Keystone was no longer required to maintain, and timely and accurately notify them if their Private Information was compromised.

K. Plaintiffs' and Class Members damages

157. To date, Keystone has done nothing to provide Plaintiffs and Class Members with relief for the damages they have suffered as a result of the Data Breach. Keystone only offered credit monitoring services to "those who are eligible," but it did not disclose how it determined eligibility. Not only did Keystone fail to provide any ongoing credit monitoring or identity protection services for all individuals impacted by the Data Breach, but the credit monitoring does nothing to compensate Class Members for damages incurred and time spent dealing with the Data Breach.

158. Plaintiffs and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

[55] *Id.*

159. As a direct and proximate result of Keystone's conduct, Plaintiffs and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. Plaintiffs and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

160. Plaintiff sand Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to target such schemes more effectively to Plaintiffs and Class members.

161. Plaintiffs and Class Members have and will also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

162. Plaintiffs and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Reviewing and monitoring financial and other sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with reporting agencies;

d. Spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;

e. Contacting financial institutions and closing or modifying financial accounts; and

f. Closely reviewing and monitoring Social Security Number, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

163. Plaintiffs and Class Members suffered actual injury from having their Private Information compromised as a result of the Data Breach including, but not limited to: (a) damage to and diminution in the value of their Private Information, a form of property that Keystone obtained from Plaintiffs and Class members; (b) violation of their privacy rights; (c) imminent and impending injury arising from the increased risk of identity theft and fraud; and (d) emotional distress.

164. Further, as a result of Defendant's conduct, Plaintiffs and Class Members are forced to live with the anxiety that their Private Information may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy with respect to that information.

165. As a direct and proximate result of Defendant's actions and inactions, Plaintiffs and Class Members have suffered a loss of privacy and are at a present and imminent and increased risk of future harm.

166. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing Private Information is not accessible online, is properly encrypted, and that access to such data is password protected.

167. Many failures laid the groundwork for the occurrence of the Data Breach, starting with Defendant's failure to incur the costs necessary to implement adequate and reasonable cyber security training, procedures and protocols that were necessary to protect Plaintiffs' and Class Members' Private Information.

168. Defendant maintained the Private Information in an objectively reckless manner, making the Private Information vulnerable to unauthorized disclosure.

169. Defendant knew, or reasonably should have known, of the importance of safeguarding Private Information and of the foreseeable consequences that would result if Plaintiffs' and Class Members' Private Information was stolen, including

the significant costs that would be placed on Plaintiffs and Class Members as a result of a breach.

170. The risk of improper disclosure of Plaintiffs' and Class Members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take necessary steps to secure Plaintiffs' and Class Members' Private Information from that risk left the Private Information in a dangerous condition.

171. Defendant disregarded the rights of Plaintiffs and Class Members by, *inter alia*, (i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that the Private Information was protected against unauthorized intrusions; (ii) failing to disclose that it did not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiffs' and Class Members' Private Information; (iii) failing to take standard and reasonably available steps to prevent the Data Breach; (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (v) failing to provide Plaintiffs and Class members prompt and accurate notice of the Data Breach.

CLASS ALLEGATIONS

172. Plaintiffs bring this class action on behalf of themselves and all members of the following Class of similarly situated persons pursuant to Federal

Rule of Civil Procedure 23:

> Nationwide Class: All persons in the United States whose Private Information was compromised in the Data Breach disclosed by Keystone on or about October 14, 2022, including all who were sent notice of the Data Breach.

173. Alternatively, or in addition to the Nationwide Class, Plaintiffs seek to represent the following State class:

> Pennsylvania Class: All persons in the commonwealth of Pennsylvania whose Private Information was compromised in the Data Breach disclosed by Keystone on or about October 14, 2022, including all who were sent notice of the Data Breach.

174. The Nationwide Class and the Pennsylvania Class are collectively referred to as the "Class." Excluded from the Class is Keystone and its affiliates, parents, subsidiaries, officers, agents, and directors, as well as the judge(s) presiding over this matter and the clerks of said judge(s).

175. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

176. Numerosity: The members in the Class are so numerous that joinder of all Class members in a single proceeding would be impracticable. As noted above, Keystone reported that approximately 235,237 individuals' information was exposed in the Data Breach.

177. Commonality and Predominance: Common questions of law and fact exist as to all Class members and predominate over any potential questions affecting only individual Class members. Such common questions of law or fact include, *inter alia*:

a. Whether Keystone had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiffs' and Class Members' PII/PHI from unauthorized access and disclosure;

b. Whether Keystone's computer systems and data security practices used to protect Plaintiffs's and Class Members' Private Information violated the FTC Act and/or HIPAA, and/or state laws and/or Keystone's other duties discussed herein;

c. Whether Keystone failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiffs and Class Members;

d. Whether Plaintiffs and Class Members suffered injury as a proximate result of Keystone's negligent actions or failures to act;

e. Whether Keystone failed to exercise reasonable care to secure and safeguard Plaintiffs' and Class Members' Private Information;

f. Whether an implied contract existed between Class members and Keystone providing that Keystone would implement and maintain reasonable security measures to protect and secure Class Members' Private Information from unauthorized access and disclosure;

g. Whether injunctive relief is appropriate and, if so, what injunctive relief is necessary to redress the imminent and currently ongoing harm faced by Plaintiffs and Class Members;

h. Whether Keystone's actions and inactions alleged herein constitute gross negligence;

i. Whether Keystone breached its duties to protect Plaintiffs' and Class members' Private Information; and

j. Whether Plaintiffs and all other members of the Class are entitled to damages and the measure of such damages and relief.

178. Keystone engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs on behalf of themselves and all other Class members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

179. Typicality: Plaintiffs' claims are typical of the claims of the Class. Plaintiff, like all proposed members of the Class, had their Private Information compromised in the Data Breach. Plaintiffs and Class Members were injured by the same wrongful acts, practices, and omissions committed by Keystone, as described herein. Plaintiffs' claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class Members.

180. Adequacy: Plaintiffs will fairly and adequately protect the interests of the Class Members. Plaintiffs are an adequate representative of the Class in their have no interests adverse to, or conflict with, the Class they seeks to represent. Plaintiffs have retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

181. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages and other financial detriment suffered by Plaintiffs and all other Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Keystone, so it would be impracticable for Class members to individually seek redress from Keystone's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments, and

increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

COUNT I
NEGLIGENCE

182. Plaintiffs reallege and incorporates by reference all preceding paragraphs as if fully set forth herein.

183. Keystone owed a duty to Plaintiffs and all other Class members to exercise reasonable care in safeguarding and protecting their PII/PHI in its possession, custody, or control.

184. Keystone knew, or should have known, the risks of collecting and storing Plaintiffs' and all other Class members' Private Information and the importance of maintaining secure systems. Keystone knew, or should have known, of the many data breaches that targeted healthcare providers in recent years.

185. Given the nature of Keystone's business, the sensitivity and value of the Private Information it maintains, and the resources at its disposal, Keystone should have identified the vulnerabilities to its systems and prevented the Data Breach from occurring.

186. Keystone breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' Private Information

by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Private Information entrusted to it—including Plaintiffs' and Class members' Private Information.

187. It was reasonably foreseeable to Keystone that its failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' Private Information by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiffs' and Class members' Private Information to unauthorized individuals.

188. But for Keystone's negligent conduct or breach of the above-described duties owed to Plaintiffs and Class members, their Private Information would not have been compromised.

189. As a result of Keystone's above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and all other Class members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—risks justifying

expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and (vii) actual or attempted fraud.

COUNT II
NEGLIGENCE PER SE

190. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

191. Keystone's duties arise from, *inter alia*, the HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and E, and the HIPAA Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C (collectively, "HIPAA Privacy and Security Rules").

192. Keystone's duties also arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by a

business, such as Keystone, of failing to employ reasonable measures to protect and secure Private Information.

193. Keystone's duties further arise from the Health Insurance Portability and Accountability Act of 1996 (HIPAA), 42 U.S.C. § 1302(d), *et seq.*

194. Keystone is an entity covered under HIPAA, which sets minimum federal standards for privacy and security of PHI.

195. Keystone violated HIPAA Privacy and Security Rules and Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiffs' and all other Class members' Private Information and not complying with applicable industry standards. Keystone's conduct was particularly unreasonable given the nature and amount of Private Information it obtains and stores, and the foreseeable consequences of a data breach involving Private Information including, specifically, the substantial damages that would result to Plaintiff and the other Class members.

196. Keystone's violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA constitutes negligence per se.

197. Plaintiffs and Class members are within the class of persons that HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to protect.

198. The harm occurring as a result of the Data Breach is the type of harm HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to

guard against.

199. It was reasonably foreseeable to Keystone that its failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' Private Information by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiffs' and Class members' Private Information to unauthorized individuals.

200. The injury and harm that Plaintiffs and the other Class members suffered was the direct and proximate result of Keystone's violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA. Plaintiffs and Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their Private Information; (iii) breach of the confidentiality of their Private Information; (iv) deprivation of the value of their Private Information, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks

of medical identity theft they face and will continue to face; and (vi) actual or attempted fraud.

COUNT III
BREACH OF FIDUCIARY DUTY

201. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

202. Plaintiffs and Class members either directly or indirectly gave Keystone their Private Information in confidence, believing that Keystone would protect that information. Plaintiffs and Class members would not have provided Keystone with this information had they known it would not be adequately protected. Keystone's acceptance and storage of Plaintiffs' and Class members' Private Information created a fiduciary relationship between Keystone and Plaintiffs and Class members. In light of this relationship, Keystone must act primarily for the benefit of its patients and health plan participants, which includes safeguarding and protecting Plaintiffs' and Class members' Private Information.

203. Keystone has a fiduciary duty to act for the benefit of Plaintiffs and Class members upon matters within the scope of their relationship. It breached that duty by failing to properly protect the integrity of the system containing Plaintiffs' and Class members' Private Information, failing to comply with the data security guidelines set forth by HIPAA, and otherwise failing to safeguard the Private Information of Plaintiffs and Class members it collected.

204. As a direct and proximate result of Keystone's breaches of its fiduciary duties, Plaintiffs and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their Private Information which remains in Keystons's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the Private Information compromised as a result of the Data Breach; and (vii) actual or attempted fraud.

COUNT IV
UNJUST ENRICHMENT

205. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein. This claim is pled in the alternative pursuant to Fed. R. Civ. P. 8(d).

206. Plaintiffs and Class members conferred a monetary benefit upon Keystone in the form of monies paid for healthcare services or other services.

207. Keystone accepted or had knowledge of the benefits conferred upon it by Plaintiffs and Class members. Keystone also benefitted from the receipt of Plaintiffs' and Class members' PHI.

208. As a result of Keystone's conduct, Plaintiffs and Class members suffered actual damages in an amount equal to the difference in value between their payments made with reasonable data privacy and security practices and procedures that Plaintiffs and Class members paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

209. Keystone should not be permitted to retain the money belonging to Plaintiffs and Class members because Keystone failed to adequately implement the data privacy and security procedures for itself that Plaintiffs and Class members paid for and that were otherwise mandated by federal, state, and local laws. and industry standards.

210. Keystone should be compelled to provide for the benefit of Plaintiffs and Class members all unlawful proceeds received by it as a result of the conduct and Data Breach alleged herein.

COUNT V
BREACH OF IMPLIED CONTRACT

211. Plaintiffs incorporate by reference all allegations of the preceding factual allegations as though fully set forth herein.

212. Defendant required Plaintiffs and Class members to provide, or authorize the transfer of, their Private Information in order for Keystone to provide services. In exchange, Defendant entered into implied contracts with Plaintiffs and Class members in which Defendant agreed to comply with its statutory and common

law duties to protect Plaintiffs' and Class members' Private Information and to timely notify them in the event of a data breach.

213. Plaintiffs and Class members would not have provided their Private Information to Defendant had they known that Defendant would not safeguard their Private Information, as promised, or provide timely notice of a data breach.

214. Plaintiffs and Class members fully performed their obligations under their implied contracts with Defendant.

215. Defendant breached the implied contracts by failing to safeguard Plaintiffs' and Class members' Private Information and by failing to provide them with timely and accurate notice of the Data Breach.

216. The losses and damages Plaintiffs and Class members sustained (as described above) were the direct and proximate result of Defendant's breach of its implied contracts with Plaintiffs and Class members.

COUNT VII
DECLARATORY AND INJUNCTIVE RELIEF

217. Plaintiffs incorporate by reference the foregoing factual allegations as if fully set forth herein.

218. This count is brought under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

219. Defendant owes a duty of care to Plaintiffs and Class members that require it to adequately secure Plaintiffs' and Class members' Private Information.

220. Defendant still possesses the Private Information of Plaintiffs and the Class members.

221. Defendant has not satisfied its contractual obligations and legal duties to Plaintiffs and the Class Members.

222. Actual harm has arisen in the wake of the Data Breach regarding Defendant's contractual obligations and duties of care to provide security measures to Plaintiffs and Class Members. Further, Plaintiffs and Class members are at risk of additional or further harm due to the exposure of their Private Information and Defendant's failure to address the security failings that led to such exposure.

223. There is no reason to believe that Defendant's employee training and security measures are any more adequate now than they were before the breach to meet Defendant's contractual obligations and legal duties.

224. Plaintiffs therefore, seeks a declaration (1) that Defendant's existing data security measures do not comply with its contractual obligations and duties of care to provide adequate data security, and (2) that to comply with its contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to, the following:

a. Ordering that Defendant engage internal security personnel to conduct testing, including audits on Defendant's systems, on a periodic basis,

and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Defendant audit, test, and train its security personnel and employees regarding any new or modified data security policies and procedures;

d. Ordering that Defendant purge, delete, and destroy, in a reasonably secure manner, any Private Information not necessary for its provision of services;

e. Ordering that Defendant conduct regular database scanning and security checks; and

f. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel and employees how to safely share and maintain highly sensitive personal information, including but not limited to, patient personally identifiable information and patient protected health information.

PRAYER FOR RELIEF

Plaintiffs, individually and on behalf of all other members of the Class, respectfully request that the Court enter judgment in their favor and against Keystone

as follows:

A. Certifying the Class as requested herein, designating Plaintiffs as Class representative, and appointing Plaintiffs' counsel as Class Counsel;

B. Awarding Plaintiffs and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement;

C. Awarding Plaintiff sand the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiffs, on behalf of themselves and the Class, seeks appropriate injunctive relief designed to prevent Keystone from experiencing another data breach by adopting and implementing best data security practices to safeguard Private Information and to provide or extend credit monitoring services and similar services to protect against all types of identity theft and medical identity theft;

D. Awarding Plaintiffs and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

E. Awarding Plaintiffs and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Awarding Plaintiffs and the Class such other favorable relief as allowable under law.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.

Dated: October 19, 2022

Respectfully submitted,

Benjamin F. Johns (PA 201373)
Samantha E. Holbrook (PA 311829)
CHIMICLES SCHWARTZ KRINER & DONALDSON-SMITH LLP
361 Lancaster Avenue
Haverford, PA 19041
Telephone: (610) 642-8500
Facsimile: (610) 649-3633
bfj@chimicles.com
seh@chimicles.com

Tina Wolfson
(*pro hac vice* forthcoming)
twolfson@ahdootwolfson.com
AHDOOT & WOLFSON, PC
2600 W. Olive Avenue, Suite 500
Burbank, CA 91505-4521
Telephone: 310.474.9111
Facsimile: 310.474.8585

Andrew W. Ferich (PA 313696)
aferich@ahdootwolfson.com
AHDOOT & WOLFSON, PC
201 King of Prussia Road, Suite 650
Radnor, PA 19087
Telephone: 310.474.9111
Facsimile: 310.474.8585

Counsel for Plaintiff and the Proposed Class